

EXHIBIT 52

Case 1:17-cv-02989-AT Document 471-7 Filed 07/10/19 Page 1 of 70



OFFICIAL ELECTION BULLETIN

September 12, 2016

TO: County Election Officials
FROM: Chris Harvey, Elections Division Director
RE: GEMS Servers and Security

In light of recent reports regarding election system security and vulnerabilities throughout the country, it is critically important that all counties preserve the security and integrity of their GEMS Server. We have previously sent updates and messages encouraging all counties to be vigilant in following existing requirements for the physical security of all election equipment, including GEMS, DREs, ExpressPolls, and other associated equipment.

With information and advice coming from many sources, it is critically important that every county remember that there should be no program, no product, no update, nor anything else added to or introduced to your GEMS Server without the direct and explicit direction of the Secretary of State's Office and/or Kennesaw State University's Center for Elections. This prohibition includes offerings, products, or solutions from local, state, or federal agencies who may be trying to provide what they feel to be assistance. Whether these solutions are described as "cyber hygiene", "virus protection" or other solutions, these programs simply cannot be introduced or added to your GEMS Server without the direct authorization of the Secretary of State or KSU.

Should any need to take any action with any election equipment arise, you will be specifically and directly contacted by the Secretary of State's Office regarding any such actions. If you ever question any communication from our office as genuine, please contact our office directly.

Again, nothing should be added to the GEMS Server without the explicit and direct instruction of the Secretary of State or KSU.

Case 1:17-cv-02989-AT Document 471-7 Filed 07/10/19 Page 3 of 70



OFFICIAL ELECTION BULLETIN

July 26, 2018

TO: County Election Officials and County Registrars
FROM: Chris Harvey, Elections Division Director
RE: Suspected Russian Operative Activity

On July 13, Special Counsel Robert Mueller released an indictment that alleges that, on or about October 28, 2016, a suspected Russian operative “visited the websites of certain counties in Georgia, Iowa, and Florida to identify vulnerabilities.”

Since the indictment was released, we have been working closely with the Department of Homeland Security to obtain more information. Now that we have more details, we are sharing with you what we have learned.

In 2016, the suspected Russian operative visited two Georgia county webpages. Those counties have been separately notified. There is no evidence that either of the county webpages were compromised as a result of this activity. Both webpages showed general, public information about elections. The federal government does not have information as to what actions the operative took in order “to identify vulnerabilities,” but they assume that the operative was conducting research designed to assist future potential operations—for example, looking for email addresses to conduct spear phishing campaigns or attempting to understand what specific technology or processes are used in our election system. The Secretary of State’s Office agrees with this assumption.

Georgia’s election systems remain secure, and we continue to prioritize our security in this environment. However, I want to remind each of you that, as election officials, you are all high-value targets. Be vigilant. Have a security mindset. Many of you have received physical security assessments from DHS, and the report is that these have been helpful. DHS also offers on-site network security assessments. On-site security assessments can be requested through ncciccusomterservice@hq.dhs.gov. The wait time for the network security assessments through DHS can be lengthy. Private sector vendors are also available without a lengthy wait. If your county wants to do a physical security or network security assessment, I will discuss the process with you and offer any support that our office can provide.

Case 1:17-cv-02989-AT Document 471-7 Filed 07/10/19 Page 5 of 70



OFFICIAL ELECTION BULLETIN

July 30, 2018

TO: County Election Officials and County Registrars
FROM: Chris Harvey, Elections Division Director
RE: Two Factor Authentication Security for ENET

As part of our continued efforts to ensure the security of the voter registration system, we are activating Two Factor Authentication for all users attempting to access the ElectioNet system beginning on Monday, July 30, 2018 at 3:30 PM. This means that after that time, all ENET users will be required to enter their password and enter an authentication code sent to their mobile number or email account when they log into the system. Detailed instructions on ElectioNet's Two Factor Authentication can be found of Firefly under Training > GVRS - eNet – ElectioNet > "Two Factor Authentication Instruction Guide." You are encouraged to review these training materials as soon as possible.

In preparation for the implementation of Two Factor Authentication in ElectioNet, we have added the ability to associate a mobile number with your eNet account. To add a mobile number to your eNet account, navigate to the My Homepage screen by selecting the icon in the top left corner of the screen labeled "My Homepage" or navigate to System > My Homepage. On this page, you can update your information by selecting the "Modify Information" button at the bottom of the screen. Be sure to select the "Save Information" button before leaving the page so that your mobile number is retained by the system.

Once you have entered a mobile number, you will notice a verify button beside your mobile number and email account. Selecting this button will send a link to your email or mobile number that allows you to verify that you have entered your information correctly. This step is required before you will be able to receive a code using that delivery method. All users are encouraged to add a mobile number to their account and verify their mobile number and email as soon as possible. Once Two Factor Authentication is activated, failure to have verified your account will result in denial of access to ENET.

Case 1:17-cv-02989-AT Document 471-7 Filed 07/10/19 Page 7 of 70



OFFICIAL ELECTION BULLETIN

August 9, 2018

TO: County Election Officials and County Registrars
FROM: Chris Harvey, Elections Division Director
RE: Physical Security Assessments Offered by Dept. of Homeland Security

This is a reminder and an encouragement for election officials to consider contacting the U.S. Department of Homeland Security (DHS) to conduct a Physical Security Assessment (PSA) on your election offices, storage facilities, or other locations in your county where election equipment or infrastructure is used or stored.

The PSAs are conducted at no cost to your county or office and can be completed in a few hours. You will be provided with suggestions for improvements to your already existing security systems and protocols.

Many counties of various sizes and resources have already taken advantage of this program, and I have heard very positive feedback about the process and interaction with DHS on these PSAs.

Dennis Mott, from DHS, is looking forward to hearing from all counties that are interested in completing a PSA in the lead-up to the 2018 General Election.

Please contact Dennis Mott directly by phone at **202-407-2793** or by email at
dennis.mott@hq.dhs.gov

If you have questions about these PSAs or other security issues, please contact me directly.

Case 1:17-cv-02989-AT Document 471-7 Filed 07/10/19 Page 9 of 70



OFFICIAL ELECTION BULLETIN

August 17, 2018

TO: County Election Officials and County Registrars

FROM: Chris Harvey, Elections Division Director

RE: Phishing Attempt

On 08-17-18, at approximately 11:12 AM, the Secretary of State's anti-phishing defenses identified an email that appeared to come from Nancy Boren, Muscogee County Election Director. The email offered an opportunity to shop at Walmart and a link for the recipient to click. Our office immediately contacted Nancy Boren directly and confirmed that she had not sent the email. She had already been alerted to the suspicious email and was working with her IT office to investigate the situation.

Our office activated our incidence response plans and immediately coordinated investigative and protective efforts with all of our security partners, including those in the federal government. Our office contacted Dept. of Homeland Security and MS-ISAC to advise them of the situation, and we took additional measures to make sure that ENET was secure. In addition, we sent out Buzz Posts and emails to county election officials to be on the alert for that or any other suspicious emails.

Muscogee County IT is working with the Department of Homeland Security and MS-ISAC to determine the nature and source of the apparent phishing attempt. Early indicators are that this was not specifically targeting the Muscogee County Elections Office.

This is a timely reminder that email phishing attempts remain one of the more popular and effective methods of cyber attack. It is imperative that all county offices train their employees on the nature of email phishing attempts and to exercise great care when interacting with email, especially email with embedded links or attachments. The additional security features added to ENET, such as two-factor authentication, continue to provide protection for ENET and other cyber systems, but the individual user still must use consistent caution when interacting with others through email and other cyber communications.

If you have questions about this situation, please contact the Secretary of State's Office.

Case 1:17-cv-02989-AT Document 471-7 Filed 07/10/19 Page 11 of 70

UNCLASSIFIED//FOR OFFICIAL USE ONLY



**Homeland
Security**

Intelligence Enterprise



INTELLIGENCE NOTE

3 October 2018

(U//FOUO) Cybersecurity – Elections, Unattributed Network Activity

(U//FOUO) Unattributed Cyber Actors Attempt to Gain Access to City Government Network Prior to Primary Election Voting

(U//FOUO) Scope. This Intelligence Note provides recent intelligence and technical indicators related to malicious activity by unattributed cyber actors, indicating possible attempts to interfere with state election infrastructure or processes. I&A prepared this Note for state and local government network defenders and elections officials.

(U//FOUO) Prepared by the Office of Intelligence and Analysis (I&A), Cyber Mission Center (CYMC). Coordinated with the National Cybersecurity and Communications Integration Center (NCCIC).

(U//FOUO) City Government Computer System Experiences Large Volume of Unauthorized Login Attempts

(U//FOUO) Unattributed cyber actors from 7 to 13 August 2018—the week prior to primary election voting—made at least 1,000 daily attempts to obtain unauthorized access to a server belonging to a Midwestern city government, according to a DHS report derived from a state law-enforcement official with direct and indirect access to cyber information.¹ In one 24-hour period during this timeframe, the actors used at least 615 unique Internet Protocol (IP) addresses to make 1,118 unauthorized login attempts, according to the same report. This state administers elections at the municipal level, which is where the described activity took place. The targeted server did not store sensitive information, and no data was exfiltrated during these events, according to the same report.

(U) Support to Computer Network Defense

(U//FOUO) The 615 IP addresses identified in that 24-hour period made at least one or more unauthorized login attempts. Of the 615 IP addresses, 4 resolved to the United States, while the remainder resolved to China (445), Brazil (42), Republic of Korea (17), India (13), Egypt (11), Russia (9), and 37 other countries, according to the same report. The chart on the following page lists the suspicious IP addresses, along with country of origin and number of access attempts associated with each. No city personnel were traveling outside the United States at the time of the incident, according to the same report.

IA-30417-19

(U) Warning: This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 USC 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with critical infrastructure and key resource personnel or private sector security officials without further approval from DHS.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Case 1:17-cv-02989-AT Document 471-7 Filed 07/10/19 Page 12 of 70

UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U//FOUO) IP Addresses Associated with Malicious Login Attempts

Country	IP Address	Number of Access Attempts
Angola	41[.]210[.]223[.]10	2
Argentina	190[.]210[.]182[.]93	4
	132[.]255[.]226[.]18	4
Australia	203[.]41[.]236[.]130	1
	47[.]74[.]66[.]207	2
Belgium	81[.]82[.]223[.]109	1
Bolivia	192[.]223[.]94[.]132	2
	200[.]58[.]160[.]67	3
Brazil	186[.]215[.]199[.]65	3
	138[.]97[.]91[.]18	1
	187[.]58[.]132[.]251	3
	189[.]114[.]67[.]213	2
	186[.]215[.]198[.]137	1
	187[.]58[.]134[.]57	4
	201[.]48[.]167[.]171	2
	186[.]215[.]199[.]219	4
	189[.]59[.]69[.]3	1
	138[.]97[.]241[.]168	2
	187[.]58[.]151[.]15	1
	186[.]215[.]143[.]149	1
	186[.]248[.]75[.]23	1
	186[.]232[.]141[.]145	1
	186[.]215[.]199[.]69	3
	177[.]43[.]244[.]209	1
	152[.]249[.]245[.]68	4
	179[.]184[.]113[.]95	1
	186[.]215[.]130[.]242	1
	177[.]159[.]99[.]31	2
	177[.]131[.]110[.]4	3
	189[.]59[.]15[.]81	1
	177[.]135[.]101[.]101	1
	189[.]59[.]15[.]91	1
	201[.]47[.]252[.]79	1
	186[.]232[.]141[.]2	1
	189[.]44[.]177[.]5	1
	186[.]249[.]13[.]250	1
	179[.]184[.]23[.]195	2

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Case 1:17-cv-02989-AT Document 471-7 Filed 07/10/19 Page 13 of 70

UNCLASSIFIED//FOR OFFICIAL USE ONLY

	177[.]135[.]101[.]93	2
	200[.]175[.]104[.]101	2
	177[.]43[.]247[.]139	1
	177[.]43[.]251[.]139	1
	177[.]43[.]243[.]231	1
	179[.]184[.]115[.]3	1
	189[.]114[.]95[.]17	1
	200[.]223[.]205[.]138	1
	186[.]215[.]199[.]223	1
	143[.]208[.]79[.]162	1
	177[.]43[.]251[.]153	2
	177[.]159[.]103[.]9	1
	200[.]186[.]49[.]229	1
Bulgaria	87[.]121[.]76[.]189	4
	31[.]13[.]227[.]4	6
	78[.]83[.]247[.]202	2
	78[.]83[.]105[.]149	1
Chile	200[.]29[.]136[.]155	2
	200[.]29[.]140[.]52	1
China	157[.]122[.]183[.]218	2
	218[.]89[.]38[.]239	1
	120[.]68[.]44[.]204	1
	183[.]65[.]17[.]118	4
	218[.]108[.]102[.]209	3
	125[.]65[.]109[.]75	1
	218[.]23[.]49[.]154	3
	221[.]10[.]230[.]228	1
	61[.]150[.]76[.]90	1
	61[.]158[.]188[.]21	13
	183[.]167[.]205[.]103	1
	218[.]107[.]49[.]71	5
	119[.]60[.]27[.]62	1
	118[.]144[.]83[.]130	2
	210[.]74[.]131[.]204	3
	61[.]160[.]81[.]62	1
	220[.]191[.]211[.]167	1
	202[.]110[.]187[.]146	2
	60[.]2[.]50[.]114	2
	61[.]167[.]79[.]135	2
	58[.]218[.]194[.]81	1
	183[.]161[.]35[.]38	2

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Case 1:17-cv-02989-AT Document 471-7 Filed 07/10/19 Page 14 of 70

UNCLASSIFIED//FOR OFFICIAL USE ONLY

	121[.]49[.]106[.]6	2
	182[.]140[.]131[.]130	1
	223[.]223[.]201[.]217	2
	61[.]132[.]233[.]195	3
	223[.]100[.]152[.]42	2
	125[.]46[.]81[.]195	4
	220[.]179[.]250[.]175	1
	221[.]178[.]227[.]10	1
	220[.]173[.]107[.]124	3
	112[.]25[.]220[.]99	2
	58[.]210[.]134[.]186	2
	124[.]128[.]73[.]58	4
	220[.]171[.]48[.]39	1
	61[.]177[.]60[.]140	3
	60[.]216[.]116[.]178	2
	61[.]185[.]242[.]195	1
	222[.]187[.]197[.]208	2
	123[.]232[.]119[.]21	7
	58[.]53[.]146[.]60	2
	222[.]88[.]238[.]11	1
	183[.]224[.]81[.]214	1
	221[.]212[.]58[.]242	3
	219[.]138[.]66[.]229	1
	60[.]172[.]73[.]3	1
	221[.]224[.]114[.]229	1
	221[.]224[.]2[.]202	1
	119[.]29[.]191[.]40	1
	119[.]90[.]34[.]135	1
	112[.]24[.]104[.]236	1
	220[.]164[.]2[.]61	2
	202[.]109[.]164[.]31	2
	183[.]214[.]89[.]122	1
	60[.]172[.]69[.]66	2
	222[.]191[.]233[.]238	2
	61[.]148[.]196[.]114	5
	220[.]164[.]2[.]113	1
	222[.]189[.]186[.]67	2
	222[.]89[.]231[.]12	1
	60[.]173[.]149[.]204	1
	121[.]28[.]40[.]179	1
	203[.]191[.]145[.]46	1

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Case 1:17-cv-02989-AT Document 471-7 Filed 07/10/19 Page 15 of 70

UNCLASSIFIED//FOR OFFICIAL USE ONLY

61[.]191[.]252[.]218	2
112[.]91[.]108[.]190	4
210[.]21[.]86[.]253	3
222[.]162[.]70[.]249	2
182[.]131[.]125[.]7	2
61[.]150[.]76[.]201	1
60[.]171[.]110[.]17	2
112[.]23[.]7[.]88	1
139[.]199[.]72[.]40	1
58[.]222[.]105[.]114	4
218[.]75[.]148[.]181	1
220[.]174[.]209[.]154	1
221[.]131[.]86[.]182	1
222[.]33[.]117[.]102	2
221[.]12[.]137[.]6	2
219[.]159[.]229[.]115	2
60[.]166[.]12[.]117	5
60[.]175[.]71[.]194	3
218[.]28[.]234[.]53	2
182[.]106[.]216[.]4	1
117[.]40[.]236[.]179	1
60[.]166[.]60[.]26	3
59[.]50[.]104[.]194	2
222[.]84[.]118[.]83	1
219[.]131[.]197[.]26	1
112[.]113[.]241[.]17	2
220[.]164[.]193[.]238	2
221[.]130[.]130[.]238	1
112[.]16[.]214[.]182	1
222[.]35[.]21[.]206	1
124[.]207[.]57[.]146	1
219[.]138[.]244[.]91	3
118[.]112[.]183[.]204	2
218[.]65[.]220[.]48	1
59[.]39[.]92[.]162	1
115[.]238[.]247[.]228	4
115[.]236[.]24[.]10	1
116[.]249[.]127[.]11	1
218[.]29[.]219[.]18	2
218[.]201[.]83[.]148	1
119[.]90[.]40[.]171	1

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Case 1:17-cv-02989-AT Document 471-7 Filed 07/10/19 Page 16 of 70

UNCLASSIFIED//FOR OFFICIAL USE ONLY

222[.]161[.]229[.]55	1
120[.]209[.]71[.]14	1
218[.]22[.]187[.]66	1
221[.]224[.]25[.]26	1
111[.]85[.]27[.]126	1
116[.]228[.]90[.]9	3
220[.]163[.]114[.]226	2
117[.]35[.]207[.]102	2
218[.]29[.]6[.]9	2
61[.]187[.]189[.]254	1
218[.]66[.]84[.]85	1
58[.]18[.]137[.]83	6
220[.]164[.]2[.]77	1
36[.]33[.]35[.]217	2
113[.]140[.]48[.]158	1
218[.]92[.]229[.]178	1
61[.]189[.]47[.]93	2
220[.]164[.]2[.]114	1
123[.]234[.]215[.]242	3
124[.]227[.]119[.]248	2
220[.]178[.]107[.]242	1
122[.]139[.]5[.]237	2
59[.]45[.]222[.]24	1
1[.]202[.]178[.]154	1
61[.]178[.]74[.]27	1
119[.]11[.]98[.]121	1
222[.]217[.]221[.]179	2
222[.]223[.]56[.]116	1
61[.]50[.]130[.]146	4
218[.]28[.]50[.]51	1
114[.]251[.]196[.]28	1
61[.]163[.]196[.]149	1
58[.]242[.]164[.]10	2
60[.]173[.]133[.]229	1
218[.]201[.]14[.]134	2
112[.]26[.]82[.]52	1
219[.]148[.]39[.]134	1
219[.]142[.]25[.]106	1
218[.]22[.]148[.]100	3
58[.]19[.]204[.]129	4
210[.]82[.]28[.]41	4

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Case 1:17-cv-02989-AT Document 471-7 Filed 07/10/19 Page 17 of 70

UNCLASSIFIED//FOR OFFICIAL USE ONLY

	220[.]163[.]44[.]182	2
	61[.]158[.]186[.]84	2
	218[.]22[.]235[.]138	1
	218[.]64[.]77[.]62	1
	223[.]241[.]100[.]16	2
	218[.]92[.]237[.]2	3
	58[.]220[.]234[.]18	1
	124[.]161[.]35[.]88	4
	222[.]185[.]255[.]227	1
	58[.]211[.]169[.]50	1
	61[.]177[.]81[.]158	2
	61[.]143[.]130[.]162	2
	122[.]226[.]136[.]90	1
	218[.]22[.]129[.]38	1
	112[.]4[.]172[.]182	1
	202[.]96[.]199[.]157	1
	220[.]174[.]241[.]102	1
	60[.]247[.]92[.]186	2
	222[.]169[.]186[.]242	2
	220[.]164[.]2[.]123	1
	60[.]2[.]111[.]190	3
	116[.]112[.]207[.]235	2
	112[.]26[.]80[.]145	1
	61[.]185[.]137[.]161	1
	218[.]29[.]52[.]2	1
	60[.]255[.]181[.]245	1
	119[.]79[.]234[.]12	3
	60[.]174[.]192[.]240	3
	61[.]160[.]95[.]126	2
	61[.]191[.]123[.]11	1
	221[.]237[.]208[.]10	1
	220[.]164[.]162[.]146	1
	58[.]213[.]133[.]18	2
	211[.]154[.]10[.]60	2
	58[.]20[.]187[.]21	6
	211[.]137[.]18[.]103	3
	61[.]233[.]18[.]34	1
	60[.]171[.]155[.]26	1
	60[.]222[.]227[.]195	1
	58[.]59[.]14[.]195	1
	221[.]226[.]176[.]254	4

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Case 1:17-cv-02989-AT Document 471-7 Filed 07/10/19 Page 18 of 70

UNCLASSIFIED//FOR OFFICIAL USE ONLY

59[.]51[.]66[.]168	1
1[.]190[.]175[.]66	3
218[.]104[.]207[.]53	4
58[.]42[.]251[.]184	2
183[.]64[.]166[.]163	2
61[.]134[.]83[.]10	1
117[.]40[.]185[.]78	1
60[.]191[.]206[.]110	1
222[.]189[.]41[.]46	1
222[.]76[.]48[.]121	1
221[.]0[.]194[.]23	5
58[.]213[.]46[.]110	1
61[.]145[.]228[.]110	2
111[.]72[.]252[.]82	1
60[.]212[.]42[.]56	8
125[.]77[.]72[.]197	1
60[.]12[.]84[.]190	1
218[.]28[.]58[.]186	1
222[.]84[.]60[.]22	1
125[.]70[.]227[.]38	2
58[.]62[.]55[.]130	1
111[.]38[.]140[.]12	2
222[.]170[.]168[.]82	1
220[.]175[.]154[.]205	1
122[.]228[.]133[.]130	1
61[.]178[.]160[.]83	1
218[.]58[.]227[.]67	4
220[.]169[.]102[.]6	1
221[.]199[.]41[.]218	1
218[.]25[.]31[.]150	1
119[.]60[.]26[.]162	1
122[.]224[.]135[.]138	2
61[.]145[.]107[.]238	2
60[.]13[.]197[.]131	1
60[.]173[.]143[.]222	1
58[.]20[.]36[.]88	3
58[.]216[.]199[.]229	1
222[.]218[.]124[.]49	1
211[.]92[.]143[.]94	2
218[.]87[.]46[.]173	1
222[.]87[.]139[.]44	1

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Case 1:17-cv-02989-AT Document 471-7 Filed 07/10/19 Page 19 of 70

UNCLASSIFIED//FOR OFFICIAL USE ONLY

60[.]172[.]64[.]229	1
116[.]248[.]41[.]55	1
218[.]57[.]237[.]243	3
222[.]222[.]219[.]154	1
115[.]239[.]244[.]198	2
124[.]128[.]25[.]147	6
58[.]240[.]2[.]38	1
120[.]42[.]52[.]82	1
124[.]164[.]235[.]209	3
112[.]27[.]129[.]78	1
219[.]232[.]115[.]95	3
60[.]169[.]26[.]22	2
111[.]75[.]162[.]114	2
123[.]138[.]78[.]210	4
222[.]240[.]159[.]130	1
222[.]161[.]47[.]82	3
220[.]178[.]151[.]125	1
60[.]173[.]69[.]118	2
218[.]207[.]74[.]9	1
218[.]22[.]253[.]37	2
111[.]1[.]89[.]230	1
60[.]171[.]157[.]209	1
218[.]23[.]26[.]50	1
61[.]180[.]38[.]132	1
211[.]147[.]65[.]218	1
59[.]61[.]73[.]130	1
36[.]7[.]79[.]21	1
112[.]16[.]58[.]21	1
124[.]42[.]103[.]139	3
60[.]30[.]5[.]5	2
61[.]187[.]123[.]74	1
222[.]218[.]17[.]189	1
220[.]164[.]2[.]88	1
219[.]138[.]59[.]240	1
218[.]28[.]164[.]218	3
113[.]204[.]147[.]26	2
101[.]231[.]140[.]218	3
120[.]202[.]36[.]46	1
60[.]174[.]118[.]80	1
221[.]7[.]96[.]91	1
124[.]129[.]30[.]246	3

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Case 1:17-cv-02989-AT Document 471-7 Filed 07/10/19 Page 20 of 70

UNCLASSIFIED//FOR OFFICIAL USE ONLY

211[.]142[.]86[.]210	2
218[.]65[.]3[.]210	1
218[.]26[.]163[.]125	1
121[.]15[.]254[.]22	1
120[.]209[.]31[.]231	2
119[.]39[.]84[.]75	2
220[.]164[.]2[.]138	1
60[.]169[.]65[.]62	2
110[.]249[.]218[.]69	2
125[.]35[.]93[.]62	2
218[.]22[.]206[.]178	1
58[.]216[.]224[.]59	1
58[.]216[.]238[.]76	1
218[.]56[.]45[.]28	3
115[.]239[.]173[.]170	1
218[.]201[.]62[.]71	2
60[.]172[.]43[.]228	1
218[.]57[.]236[.]58	2
125[.]77[.]127[.]97	1
218[.]22[.]100[.]42	1
223[.]72[.]168[.]150	1
221[.]193[.]214[.]166	1
60[.]2[.]101[.]221	5
61[.]136[.]81[.]154	2
221[.]178[.]192[.]194	2
115[.]238[.]34[.]226	1
60[.]171[.]140[.]110	1
221[.]231[.]109[.]126	1
220[.]168[.]205[.]16	1
183[.]167[.]231[.]206	1
220[.]178[.]177[.]15	1
222[.]161[.]209[.]130	2
61[.]28[.]113[.]58	3
117[.]158[.]187[.]110	3
218[.]28[.]135[.]178	2
218[.]28[.]171[.]213	1
222[.]218[.]17[.]94	2
60[.]161[.]215[.]7	1
60[.]174[.]92[.]50	1
61[.]153[.]49[.]210	3
220[.]164[.]2[.]118	1

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Case 1:17-cv-02989-AT Document 471-7 Filed 07/10/19 Page 21 of 70

UNCLASSIFIED//FOR OFFICIAL USE ONLY

61[.]161[.]209[.]134	3
123[.]138[.]199[.]66	4
111[.]204[.]225[.]178	2
114[.]104[.]158[.]172	1
60[.]172[.]231[.]12	1
59[.]52[.]27[.]130	1
61[.]161[.]147[.]218	2
218[.]22[.]180[.]146	1
219[.]138[.]243[.]196	2
58[.]221[.]60[.]110	1
175[.]19[.]204[.]202	6
60[.]28[.]131[.]10	1
119[.]53[.]91[.]170	4
60[.]11[.]113[.]164	3
58[.]18[.]170[.]107	5
27[.]42[.]165[.]226	4
220[.]164[.]2[.]124	1
60[.]166[.]48[.]158	1
60[.]10[.]41[.]203	1
124[.]207[.]209[.]114	1
220[.]178[.]26[.]20	1
122[.]97[.]16[.]154	4
60[.]171[.]164[.]47	1
122[.]224[.]3[.]12	2
60[.]174[.]37[.]226	1
203[.]93[.]109[.]130	1
117[.]69[.]253[.]252	1
122[.]140[.]95[.]92	2
60[.]6[.]223[.]191	1
61[.]136[.]94[.]166	3
61[.]163[.]36[.]24	3
14[.]204[.]55[.]6	1
58[.]214[.]239[.]53	1
222[.]92[.]204[.]50	1
116[.]113[.]86[.]246	1
60[.]30[.]224[.]189	3
218[.]94[.]137[.]82	1
222[.]242[.]226[.]99	1
222[.]161[.]246[.]150	5
43[.]227[.]254[.]4	3
61[.]182[.]241[.]10	1

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Case 1:17-cv-02989-AT Document 471-7 Filed 07/10/19 Page 22 of 70

UNCLASSIFIED//FOR OFFICIAL USE ONLY

	119[.]48[.]16[.]182	5
	122[.]139[.]5[.]236	3
	111[.]26[.]198[.]30	1
	58[.]19[.]182[.]235	4
	58[.]22[.]194[.]44	3
	58[.]214[.]24[.]53	1
	220[.]189[.]205[.]2	1
	60[.]13[.]181[.]244	2
	60[.]13[.]3[.]26	6
	61[.]158[.]140[.]152	1
	220[.]164[.]2[.]91	1
	117[.]28[.]250[.]42	4
	42[.]228[.]1[.]34	5
	60[.]216[.]106[.]162	2
	218[.]58[.]105[.]206	2
	218[.]26[.]97[.]162	1
	222[.]141[.]50[.]134	2
	219[.]154[.]133[.]161	3
	221[.]210[.]134[.]161	1
	112[.]91[.]59[.]106	1
	221[.]212[.]18[.]146	1
	219[.]154[.]66[.]223	1
	218[.]24[.]236[.]4	1
	58[.]244[.]188[.]78	1
	218[.]200[.]55[.]214	1
	122[.]195[.]155[.]194	1
	111[.]206[.]163[.]56	3
	221[.]4[.]205[.]30	2
	61[.]53[.]66[.]4	3
	123[.]7[.]54[.]235	1
	61[.]163[.]229[.]226	1
	171[.]221[.]226[.]23	1
	122[.]227[.]185[.]67	2
	221[.]210[.]83[.]24	3
	60[.]223[.]252[.]6	2
	61[.]136[.]81[.]234	1
	218[.]94[.]144[.]101	3
	119[.]53[.]149[.]66	1
	221[.]3[.]236[.]94	1
	61[.]182[.]27[.]121	2
	221[.]176[.]176[.]126	1

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Case 1:17-cv-02989-AT Document 471-7 Filed 07/10/19 Page 23 of 70

UNCLASSIFIED//FOR OFFICIAL USE ONLY

110[.]17[.]188[.]30	1
58[.]20[.]185[.]12	2
218[.]27[.]162[.]22	2
124[.]165[.]247[.]42	1
61[.]136[.]104[.]131	3
60[.]6[.]214[.]48	2
221[.]207[.]20[.]154	1
61[.]163[.]69[.]170	1
60[.]30[.]66[.]199	3
113[.]8[.]194[.]3	1
116[.]113[.]96[.]22	1
221[.]230[.]11[.]113	1
122[.]225[.]238[.]98	1
221[.]7[.]133[.]28	1
218[.]56[.]102[.]14	1
116[.]228[.]50[.]194	1
60[.]6[.]227[.]95	1
210[.]73[.]8[.]244	1
60[.]167[.]19[.]30	1
120[.]237[.]228[.]16	2
218[.]64[.]165[.]194	1
111[.]38[.]216[.]5	1
218[.]22[.]66[.]30	1
111[.]113[.]11[.]82	1
222[.]186[.]68[.]154	1
221[.]2[.]157[.]133	1
222[.]243[.]211[.]200	1
221[.]4[.]197[.]154	1
60[.]8[.]207[.]34	1
61[.]178[.]243[.]56	1
218[.]204[.]69[.]3	1
124[.]112[.]193[.]26	1
58[.]210[.]126[.]206	1
123[.]172[.]215[.]62	1
120[.]209[.]115[.]132	1
218[.]28[.]76[.]99	1
218[.]3[.]210[.]2	1
218[.]23[.]162[.]169	1
58[.]214[.]25[.]190	1
221[.]202[.]201[.]85	1
220[.]164[.]2[.]100	1

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Case 1:17-cv-02989-AT Document 471-7 Filed 07/10/19 Page 24 of 70

UNCLASSIFIED//FOR OFFICIAL USE ONLY

	221[.]239[.]8[.]178	1
	113[.]240[.]237[.]10	1
	220[.]163[.]44[.]185	1
	58[.]216[.]156[.]58	1
	218[.]241[.]156[.]10	1
	60[.]172[.]22[.]178	1
	61[.]134[.]52[.]164	1
	36[.]33[.]0[.]160	1
	218[.]104[.]133[.]243	1
	61[.]136[.]82[.]164	1
	112[.]24[.]104[.]228	1
	221[.]131[.]83[.]162	1
Colombia	190[.]60[.]31[.]185	2
	190[.]90[.]41[.]234	1
	201[.]184[.]241[.]243	3
Czech Republic	90[.]179[.]120[.]155	3
	90[.]183[.]127[.]106	4
	85[.]70[.]69[.]194	4
Denmark	85[.]191[.]101[.]60	5
Egypt	41[.]41[.]160[.]186	1
	197[.]50[.]15[.]189	3
	41[.]128[.]185[.]155	2
	197[.]50[.]105[.]120	1
	196[.]219[.]154[.]248	1
	41[.]39[.]155[.]221	1
	197[.]44[.]214[.]61	2
	197[.]45[.]1[.]118	1
	41[.]38[.]128[.]154	2
	41[.]39[.]153[.]128	1
	41[.]41[.]30[.]169	1
	80[.]147[.]59[.]28	2
	41[.]242[.]139[.]222	2
Germany	190[.]56[.]70[.]131	1
Jordan	82[.]212[.]83[.]154	4
India	182[.]74[.]165[.]174	4
	220[.]225[.]7[.]27	1
	220[.]225[.]7[.]91	5
	42[.]104[.]94[.]237	5
	220[.]225[.]7[.]21	1
	220[.]225[.]7[.]45	4
	220[.]225[.]7[.]46	1

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Case 1:17-cv-02989-AT Document 471-7 Filed 07/10/19 Page 25 of 70

UNCLASSIFIED//FOR OFFICIAL USE ONLY

	223[.]30[.]252[.]114	1
	220[.]225[.]7[.]49	1
	220[.]227[.]147[.]150	2
	220[.]225[.]7[.]31	2
	182[.]74[.]92[.]178	1
	220[.]225[.]7[.]19	1
Indonesia	203[.]142[.]65[.]102	1
	114[.]199[.]112[.]138	1
	202[.]93[.]35[.]19	2
Israel	109[.]226[.]23[.]26	1
	213[.]57[.]176[.]22	3
Italy	62[.]149[.]211[.]160	1
	88[.]32[.]17[.]110	1
	62[.]86[.]183[.]89	1
	80[.]19[.]218[.]22	1
Japan	220[.]102[.]99[.]96	1
	222[.]229[.]112[.]168	1
Laos	115[.]84[.]112[.]138	5
	202[.]137[.]141[.]81	7
	115[.]84[.]105[.]146	1
Malaysia	175[.]143[.]104[.]25	1
	201[.]140[.]110[.]78	4
Mexico	189[.]206[.]125[.]171	1
	189[.]204[.]6[.]157	1
Pakistan	182[.]190[.]4[.]84	1
Poland	85[.]89[.]165[.]89	1
Qatar	82[.]148[.]97[.]167	2
Republic of Korea	118[.]223[.]102[.]130	3
	112[.]179[.]242[.]181	1
	211[.]232[.]116[.]145	1
	222[.]101[.]93[.]2	2
	221[.]151[.]127[.]218	1
	123[.]214[.]172[.]84	2
	61[.]37[.]150[.]6	2
	121[.]128[.]135[.]75	3
	203[.]242[.]126[.]4	2
	206[.]219[.]17[.]55	4
	211[.]232[.]116[.]146	1
	1[.]255[.]70[.]86	3
	1[.]255[.]70[.]123	1
	1[.]255[.]70[.]114	2

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Case 1:17-cv-02989-AT Document 471-7 Filed 07/10/19 Page 26 of 70

UNCLASSIFIED//FOR OFFICIAL USE ONLY

	121[.]128[.]135[.]74	1
	115[.]1[.]56[.]141	1
	112[.]218[.]211[.]227	1
Moldova	188[.]237[.]250[.]100	2
	93[.]116[.]201[.]15	2
	109[.]185[.]181[.]14	1
Romania	82[.]77[.]6[.]21	3
Russia	5[.]101[.]8[.]11	2
	188[.]235[.]6[.]85	5
	83[.]239[.]78[.]134	6
	94[.]253[.]8[.]118	1
	78[.]25[.]82[.]10	3
	46[.]229[.]65[.]152	2
	217[.]26[.]1[.]82	1
	78[.]36[.]17[.]204	1
	95[.]47[.]155[.]87	1
Serbia	188[.]255[.]255[.]163	1
Singapore	158[.]140[.]138[.]168	2
Slovakia	193[.]150[.]73[.]22	2
	217[.]119[.]114[.]106	1
	195[.]88[.]83[.]34	3
Taiwan	106[.]11[.]59[.]190	1
	118[.]163[.]97[.]19	3
	118[.]163[.]58[.]117	2
	125[.]227[.]146[.]182	4
	125[.]227[.]179[.]59	2
	118[.]163[.]143[.]170	2
	211[.]20[.]181[.]113	1
	118[.]163[.]135[.]18	2
Thailand	122[.]155[.]202[.]169	1
	210[.]86[.]168[.]116	1
Turkey	185[.]59[.]75[.]47	3
Ukraine	109[.]254[.]8[.]169	1
United Arab Emirates	83[.]110[.]55[.]14	1
United Kingdom	109[.]170[.]184[.]211	4
	77[.]44[.]110[.]101	4
	109[.]170[.]160[.]102	2
	109[.]170[.]160[.]109	2
United States	67[.]237[.]78[.]130	1
	216[.]59[.]166[.]113	1
	168[.]103[.]20[.]54	4

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Case 1:17-cv-02989-AT Document 471-7 Filed 07/10/19 Page 27 of 70

UNCLASSIFIED//FOR OFFICIAL USE ONLY

	50[.]252[.]166[.]69	1
Venezuela	190[.]202[.]44[.]194	1
Vietnam	14[.]177[.]235[.]133	3
	137[.]59[.]45[.]16	1

(U) Reporting Computer Security Incidents

(U) To report a computer security incident, either contact NCCIC at 888-282-0870, or go to <https://forms.us-cert.gov/report/> and complete the US-CERT Incident Reporting System form. The US-CERT Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to US-CERT. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent.

(U) Tracked by: HSEC-1.1, HSEC-1.2, HSEC-1.5, HSEC-1.8

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Case 1:17-cv-02989-AT Document 471-7 Filed 07/10/19 Page 28 of 70

UNCLASSIFIED//FOR OFFICIAL USE ONLY

¹ (U//FOUO); DHS; IIR 4 007 0540 18; 150031Z AUG 2018; DOI 13 AUG 2018; (U//FOUO); Midwestern City Government Computer System Experiencing a Large Volume of Malicious Login Attempts Prior to Primary Election Voting; Extracted information is U//FOUO; Overall document classification is U//FOUO.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Page 18 of 18

Case 1:17-cv-02989-AT Document 471-7 Filed 07/10/19 Page 29 of 70

UNCLASSIFIED//FOR OFFICIAL USE ONLY



**Homeland
Security**

Intelligence Enterprise



INTELLIGENCE NOTE

4 October 2018

(U) Cybersecurity – Elections, Unattributed Cyber Activity

(U//FOUO) Unattributed Cyber Actors Spoof Senior State Election Official's E-mail, Spear Phish City Clerk

(U//FOUO) Scope. This *Intelligence Note* provides recent intelligence and technical indicators from malicious activity by unattributed cyber actors that occurred prior to a US state's primary election, indicating possible attempts to interfere with state election infrastructure or processes. I&A prepared this *Note* for state and local government network defenders and elections officials.

(U//FOUO) Prepared by the DHS Intelligence Enterprise (DHS IE), Cyber Mission Center (CYMC). Coordinated with the National Cybersecurity and Communications Integration Center (NCCIC).

(U//FOUO) Spoofing of Senior State Election Official's E-mail for Spear Phishing

(U//FOUO) An unknown cyber actor on 5 July 2018 spoofed the e-mail address of the second highest ranking official in a state government elections organization to send a malicious spear-phishing e-mail to a city clerk-treasurer in the same state; however, no breach or data exfiltration occurred, according to DHS reporting derived from a state employee with direct access to cybersecurity information through support to a US state's election-related information technology systems.¹ The state issued a press release before this event announcing the state official's promotion to the number two position in the state elections organization and that the official has led the state's accessibility initiatives as well as voting equipment testing and auditing programs, among other initiatives, according to the same report. Elections in this state are administered at the municipal level, which is where the described activity occurred, according to the same report.

(U//FOUO) The e-mail used an "invoice"-themed subject, malicious hyperlink, and an Internet Protocol address that resolved to Mexico (187[.]188[.]177[.]218), according to the same report. Anti-phishing software removed a known bad hyperlink from the e-mail message, deleted or quarantined the malicious hyperlink, and replaced it with a notification message to the city clerk-treasurer, according to the report. No breach or data exfiltration occurred. The city clerk-treasurer notified the state election official that his identity was being used in a spear-phishing attempt, according to the report.

IA-30352-19

(U) **Warning:** This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with critical infrastructure and key resource personnel or private sector security officials without further approval from DHS.

(U) US person information has been minimized. Should you require the minimized US person information, please contact the I&A Production Branch at IA.PM@dhs.gov or IA.PM@dhs.ic.gov.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Case 1:17-cv-02989-AT Document 471-7 Filed 07/10/19 Page 30 of 70

UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U//FOUO) Support to Computer Network Defense

(U//FOUO) Image of Spear-Phishing E-mail²

UNCLASSIFIED//FOR OFFICIAL USE ONLY

-----Original Message-----

From: Lastname
Sent: Thursday, July 5, 2018 12:00 PM
To: Firstname Lastname, Clerk-Treasurer
<firstname.lastname@citynametwoletterstateabbreviation.gov>
Subject: Customer Invoice FO 4421502

Have you had a chance to review the invoice I sent last week? I'm sending it again.

USPER Business Agent Anti-phishing removed a known bad URL from your email message. It was deleted or quarantined and replaced with this message.

Yours,

Lastname, Firstname Middleinitial - XXX

(U) Reporting Computer Security Incidents

(U) To report a computer security incident, either contact NCCIC at 888-282-0870, or go to <https://forms.us-cert.gov/report/> and complete the US-CERT Incident Reporting System form. The US-CERT Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to US-CERT. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent.

(U) Tracked by: HSEC-1.1, HSEC-1.2, HSEC-1.5, HSEC-1.8

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Case 1:17-cv-02989-AT Document 471-7 Filed 07/10/19 Page 31 of 70

UNCLASSIFIED//FOR OFFICIAL USE ONLY

¹ (U//FOUO); DHS; IIR 4 007 0606 18; 131225Z SEP 2018; DOI 05 JUL-23 AUG 2018; (U//FOUO); Spoofing of Senior State Election Official Email Address to Send Spearphishing Email to City Government Official; Extracted information is U//FOUO; Overall document classification is U//FOUO.

² (U//FOUO); DHS; IIR 4 007 0606 18; 131225Z SEP 2018; DOI 05 JUL-23 AUG 2018; (U//FOUO); Spoofing of Senior State Election Official Email Address to Send Spearphishing Email to City Government Official; Extracted information is U//FOUO; Overall document classification is U//FOUO.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Case 1:17-cv-02989-AT Document 471-7 Filed 07/10/19 Page 32 of 70

CLASSIFICATION: UNCLASSIFIED//FOR OFFICIAL USE ONLY

**Homeland
Security**

Office of Intelligence and Analysis

Customer Feedback Form

Product Title: (U//FOUO) Unattributed Cyber Actors Spoof Senior State Election Official's E-mail, Spear Phish City Clerk

All survey responses are completely anonymous. No personally identifiable information is captured unless you voluntarily offer personal or contact information in any of the comment fields. Additionally, your responses are combined with those of many others and summarized in a report to further protect your anonymity.

1. Please select partner type:	Select One	and function:	Select One
2. What is the highest level of intelligence information that you receive?	Select One		
3. Please complete the following sentence: "I focus most of my time on:"	Select One		
4. Please rate your satisfaction with each of the following:			

	Very Satisfied	Somewhat Satisfied	Neither Satisfied nor Dissatisfied	Somewhat Dissatisfied	Very Dissatisfied	N/A
Product's overall usefulness	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Product's relevance to your mission	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Product's timeliness	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Product's responsiveness to your intelligence needs	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

5. How do you plan to use this product in support of your mission? (Check all that apply.)

- | | |
|--|---|
| <input type="checkbox"/> Drive planning and preparedness efforts, training, and/or emergency response operations | <input type="checkbox"/> Initiate a law enforcement investigation |
| <input type="checkbox"/> Observe, identify, and/or disrupt threats | <input type="checkbox"/> Initiate your own regional-specific analysis |
| <input type="checkbox"/> Share with partners | <input type="checkbox"/> Initiate your own topic-specific analysis |
| <input type="checkbox"/> Allocate resources (e.g. equipment and personnel) | <input type="checkbox"/> Develop long-term homeland security strategies |
| <input type="checkbox"/> Reprioritize organizational focus | <input type="checkbox"/> Do not plan to use |
| <input type="checkbox"/> Author or adjust policies and guidelines | <input type="checkbox"/> Other: _____ |

6. To further understand your response to question #5, please provide specific details about situations in which you might use this product.

7. What did this product not address that you anticipated it would?

8. To what extent do you agree with the following two statements?

	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree	N/A
This product will enable me to make better decisions regarding this topic.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
This product provided me with intelligence information I did not find elsewhere.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

9. How did you obtain this product? Select One

10. Would you be willing to participate in a follow-up conversation about your feedback? Yes

To help us understand more about your organization so we can better tailor future products, please provide:

Name: _____
 Organization: _____
 Contact Number: _____

Position: _____
 State: _____
 Email: _____

Submit Feedback

Privacy Act Statement

CLASSIFICATION: UNCLASSIFIED//FOR OFFICIAL USE ONLY

Product Serial Number: IA-30352-19

REV: 01 August 2017

Case 1:17-cv-02989-AT Document 471-7 Filed 07/10/19 Page 33 of 70
UNCLASSIFIED

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
DIRECTOR OF THE NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER
WASHINGTON, DC 20511

NCSC-18-502

MEMORANDUM FOR: The Honorable Christopher C. Krebs
Under Secretary for National Protection and Programs Directorate
Department of Homeland Security

The Honorable David J. Glawe
Under Secretary for Intelligence and Analysis
Department of Homeland Security

Mr. Joshua D. Skule
Executive Assistant Director, Intelligence Branch
Federal Bureau of Investigation

SUBJECT: **Election Security Information Needs:** Foreign Threats to U.S. Elections

The National Counterintelligence and Security Center (NCSC) is working closely with the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), the Election Assistance Commission, and other Federal agencies to assess and mitigate foreign governments' actions to interfere in U.S. elections. The Intelligence Community (IC) continuously reviews intelligence to identify foreign threats to the U.S. election infrastructure. The U.S. election infrastructure consists of (a) storage facilities, polling places, voter registration offices, and centralized vote tabulation locations used to support U.S. election processes, as well as (b) information and communications technology, including voter registration databases, voting machines, and other electronic systems used to manage U.S. election processes and display results on behalf of state and local governments. The national-level information needs we cite below are intended to be disseminated to election officials at all levels (state, local, tribal, and territorial) to help them identify, understand, report on and counter any efforts to interfere in U.S. elections. I encourage you to disseminate these information needs to election officials to the widest extent possible to encourage the reporting of suspected or confirmed threats to U.S. electoral infrastructure or election activities.

Foreign governments' efforts to interfere with U.S. elections fall into four distinct categories: (a) cyber operations targeting election infrastructure; (b) cyber operations targeting political organizations, campaigns, and public officials; (c) influence operations to assist or harm political organizations, campaigns, and public officials, or to sway public opinion and sow division; and (d) physical threats to polling places and election offices. Election officials are encouraged to report to DHS and FBI any indicators that foreign actors may be engaged in the following activities prior to, during, and following the day of the election, to include:

UNCLASSIFIED

Case 1:17-cv-02989-AT Document 471-7 Filed 07/10/19 Page 34 of 70

UNCLASSIFIED

SUBJECT: **Election Security Information Needs:** Foreign Threats to U.S. Elections

1. Unauthorized entry or attempts to gain access to long term storage facilities, polling places, and voter centers, including those that may be located on public or private property, used to store election and voting system infrastructure.
2. Incidences of spear-phishing or attempts to hack voter registration systems, to include similar efforts against seemingly unrelated state or local government entities, such as the Department of Motor Vehicles or other agencies or civic organizations responsible for registering voters.
3. Attempts to access, alter, or destroy systems used to qualify candidates; produce and deliver ballots; procure, manage and prepare voting equipment; process requests for absentee ballots; and store and manage election administration process and procedure documentation.
4. Unauthorized access, or attempts to access, IT infrastructure or systems used to manage elections, including systems that count, audit, or display election results on election night and systems used to certify and validate post-election results.
5. Attempts to hack, spear-phish, or compromise personal or professional e-mail accounts and social media accounts of elections officials, staff and volunteers.
6. Hacking attempts or successful hacks into political party headquarters or candidate IT systems.
7. Attempts to access, hack, alter, or disrupt infrastructure to receive and process absentee ballots through tabulation centers, web portals, e-mail, or fax machines; attempts to interfere with votes sent through the U.S. Postal Service.
8. Compromises of any networks and/or systems, including hardware and/or software, by cyber actors to include the tactics, techniques, procedures and impact observed on election-related networks and systems; evidence of interference detected on state networks or systems for cyber security indicators of compromise.
9. Instances of any unexplained disruption at polling stations or training locations for voting officials, including early voting locations, which block or limit voter turnout. Disruptions may include social media posts or robocalls falsely reporting closed or changed polling stations, or physical incidents at polling stations, including distribution of false information.
10. Disinformation efforts to alter or shutdown government web sites to foment social unrest or reduce voter turnout, to include on social media or other electronic means.
11. Unauthorized entry of centralized vote counting/tallying locations or electronic systems or networks used by states and localities to count absentee/military and election day voting ballots.

UNCLASSIFIED

Case 1:17-cv-02989-AT Document 471-7 Filed 07/10/19 Page 35 of 70
UNCLASSIFIED

SUBJECT: **Election Security Information Needs:** Foreign Threats to U.S. Elections

12. Impacts to critical infrastructure that limit access to polling stations such as power, water, internet, telephone (cellular), and transportation (traffic controls) outages.



William R. Evanina

7-5-18

Date

cc: see Distribution List

Case 1:17-cv-02989-AT Document 471-7 Filed 07/10/19 Page 36 of 70
UNCLASSIFIED

SUBJECT: **Election Security Information Needs:** Foreign Threats to U.S. Elections

Distribution:

Director of National Intelligence
Under Secretary of Defense for Intelligence
Director of Intelligence, J-2, Joint Chiefs of Staff
Director, Office of Intelligence and Counterintelligence, Department of Energy
Under Secretary, Office of Intelligence and Analysis, Department of Homeland Security
Assistant Secretary of State for Intelligence and Research
Assistant Secretary of the Treasury for Intelligence and Analysis
Executive Assistant Director, Intelligence Branch, Federal Bureau of Investigation
Director, Central Intelligence Agency
Director, Defense Intelligence Agency
Director, National Geospatial-Intelligence Agency
Director, National Reconnaissance Office
Director, National Security Agency
Chief of Intelligence/Senior Officer, Drug Enforcement Administration
Deputy Chief of Staff, G2, United States Army
Director of Intelligence, Headquarters, United States Marine Corps
Director of Naval Intelligence, United States Navy
Deputy Chief of Staff for Intelligence, Surveillance and Reconnaissance, United States Air Force
Assistant Commandant for Intelligence and Criminal Investigations, United States Coast Guard

Case 1:17-cv-02989-AT Document 471-7 Filed 07/10/19 Page 37 of 70

UNCLASSIFIED//FOR OFFICIAL USE ONLY

2 October 2018

(U) A Georgia Perspective on Threats to the 2018 U.S. Elections

(U) Prepared by the DHS Office of Intelligence & Analysis (DHS I&A), Field Operations Division, Southeast Region. Coordinated with the DHS I&A Cyber Mission Center.

(U//FOUO) DHS I&A assesses that foreign governments may engage in cyber operations targeting the election infrastructure and political organizations in Georgia and engage in influence operations that aim to interfere with the 2018 U.S Elections. The motives of these cyber actors and foreign influencers may vary; they may intend to disrupt political processes, sway public opinion, or to support or undermine certain political organizations. In the past month, DHS observed multiple tactics targeting election related infrastructure at the local and state level to include, but not limited to, spearphishing, Cross Site Scripting (XSS), Structured Query Language Injections (SQLI), and attempted Denial of Service (DoS) attacks.^{1,2}

(U) DHS I&A is particularly concerned about the potential for the following activities related to the 2018 U.S. election:¹

- (U) Unauthorized entry to polling places or long-term storage facilities, and voting facilities used to store election and voting system infrastructure.
- (U) Incidents of spearphishing or attempts to hack voter registration systems, such as Department of Motor Vehicles (DMV) or other organizations used to register voters.
- (U) Attempts to access information technology (IT) infrastructure used to manage elections, display results, or for counting or certifying votes.
- (U) Hacking or spearphishing attempts against the emails or social media accounts of election officials, staff or volunteers.
- (U) Hacking attempts of political party headquarters or candidate's IT systems or websites.
- (U) Attempts to hack, alter or disrupt infrastructure used to process absentee ballots or attempts to interfere with votes sent through the US Postal Service.
- (U) Compromise of any networks or systems by cyber actors, including tactics, techniques, and procedures, along with the impact observed on election-related systems.
- (U) Any unexplained disruptions at polling places or training locations which block or limit voter turnout. This may include social medial messages or robo-calls falsely reporting changed or closed polling locations, or physical incidents at polling locations, including distribution of false information.
- (U) Disinformation efforts to shut down government websites to foment social unrest or reduce voter turnout.
- (U) Impacts to critical infrastructure that limit access to polling stations, such as power outages, internet, telephone (cellular), and transportation (traffic control) outages.³

(U) Election officials are encouraged to report any activity related to the above information needs to the Georgia Secretary of State's Office.

¹ For additional elections security related resources visit <https://www.dhs.gov/publication/election-security-resources>



**Office of Intelligence & Analysis
Field Operations, Southeast Region**

(U) Warning: This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with authorized critical infrastructure and key resource personnel and private sector security officials without further approval from DHS.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Case 1:17-cv-02989-AT Document 471-7 Filed 07/10/19 Page 38 of 70

UNCLASSIFIED//FOR OFFICIAL USE ONLY

2 October 2018

¹ (U//FOUO) DHS; IIR 4 007 0590 18; (U//FOUO) Attempts to Illegally Access Online Voter Registration Database Using Structured Query Language Injections and Cross Site Scripting; Extracted Information is (U//FOUO); Overall document is (U//FOUO).

² (U//FOUO) DHS; IIR 4 007 0605 18; (U//FOUO) Spoofing of Senior State Election Official Email Address to Send Spearphishing Email to City Government Official; Extracted Information is (U//FOUO); Overall document is (U//FOUO).

³ (U) ODNI Director of the National Counterintelligence and Security Center; NSCS-18-502; (U) Election Security Information Needs: Foreign Threats to U.S. Elections; 05 SEP 2018.



*Office of Intelligence & Analysis
Field Operations, Southeast Region*

(U) Warning: This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with authorized critical infrastructure and key resource personnel and private sector security officials without further approval from DHS.

UNCLASSIFIED//FOR OFFICIAL USE ONLY